

ICS 33.040.40

CCS M 32



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 46240.2-2025

**Security requirements and testing methods of IPv6 network
equipment - Part 2: Switch**

IPv6网络设备安全技术要求和测试方法 第2部分：交换机

Issued on: August 29, 2025

Implemented on: December 1, 2025

**Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC**

Table of Contents

Preface	V
Introduction	VI
1 Scope	1
2 Normative references	1
3 Terms and Definitions	1
4 Abbreviations	1
5 General Principles	2
6 Safety Technical Requirements	3
6.1 Data Plane Security	3
6.1.1 Identification and Authentication	3
6.1.2 Trusted Channel	3
6.1.3 System Access	3
6.1.4 Resource Allocation	3
6.1.4.1 Ability to resist large-volume attacks	3
6.1.4.2 Anti-deformation package capability	4
6.1.4.3 ND Illegal Packet Attack Protection	4
6.1.4.4 IPv6 address spoofing protection	4
6.1.4.5 Multicast Packet Suppression	4
6.1.5 Security Audit	4
6.1.5.1 Attack Source Tracing Function	4
6.1.5.2 Sampling function	4
6.1.6 System Function Protection	5
6.1.7 Security Management	5
6.2 Control Plane Security	5
6.2.1 Identification and identification	5
6.2.1.1 Routing Authentication	5
6.2.1.2 ND message authentication function	5
6.2.1.3 Intelligent Lossless Storage Network Authentication	5
6.2.1.4 Cross-device link aggregation authentication	5
6.2.1.5 OpenFlow Authentication	5
6.2.2 Trusted Channel	5
6.2.3 System Access	6

6.2.4 Resource Allocation	6
6.2.4.1 MAC Address Learning Limitation	6
6.2.4.2 Disabling ICMPv6	6
6.2.4.3 Disable the Hop-by-Hop option	6
6.2.5 Security Audit	6
6.2.6 System Function Protection	6
6.2.7 Security Management	6
6.3 Management Plane Security	6
6.3.1 Identification and Authentication	6
6.3.2 Trusted Channel	6
6.3.3 System Access	7
6.3.3.1 Access Control Security	7
6.3.3.2 Serial Port Access	7
6.3.3.3 SSH Access	7
6.3.3.4 SNMP Access	7
6.3.3.5 Web Access	7
6.3.4 Resource Allocation	7
6.3.5 Security Audit	8
6.3.6 System Function Protection	8
6.3.7 Security Management	8
6.3.7.1 Hierarchical and decentralized management	8
6.3.7.2 Insecure Configuration Check	8
6.3.7.3 Digital Certificate Management	8
6.3.7.4 Password Requirements	8
7 Test Methods	8
7.1 Test Environment	8
7.2 Data Plane Security Testing	10
7.2.1 Identification and identification	10
7.2.1.1 802.1X Access Authentication Function	10
7.2.1.2 MAC access authentication function	11
7.2.1.3 MAC Address Drift Detection Function	11
7.2.2 Trusted Channel	11
7.2.3 System Access	11
7.2.4 Resource Allocation	12
7.2.4.1 Ability to resist large-volume attacks	12

7.2.4.2 Anti-deformation package capability	13
7.2.4.3 ND Illegal Packet Attack Protection	15
7.2.4.4 IPv6 address spoofing protection	15
7.2.4.5 Multicast Packet Suppression	16
7.2.5 Security Audit	16
7.2.5.1 Attack Source Tracing Function	16
7.2.5.2 Sampling function	16
7.2.6 System Function Protection	16
7.2.7 Security Management	17
7.3 Control Plane Security Testing	17
7.3.1 Identification and identification	17
7.3.1.1 Routing Authentication	17
7.3.1.2 ND message authentication function	18
7.3.1.3 Intelligent Lossless Storage Network Certification	19
7.3.1.4 Cross-device link aggregation authentication	20
7.3.1.5 OpenFlow Authentication	20
7.3.2 Trusted Channel	20
7.3.2.1 RIPng supports IPsec function	20
7.3.2.2 OSPFv3 Supports IPsec	21
7.3.2.3 BGP4 supports TLS	21
7.3.3 System Access	21
7.3.3.1 BGP4 Inbound Route Filtering	21
7.3.3.2 BGP4 Outbound Route Filtering	21
7.3.3.3 Route filtering based on BGP4 attributes	22
7.3.3.4 Route Filtering in Route Redistribution	22
7.3.4 Resource Allocation	22
7.3.4.1 MAC Address Learning Limit	22
7.3.4.2 Disabling ICMPv6 Function	23
7.3.4.3 Disabling the Hop-by-Hop Option	23
7.3.5 Security Audit	23
7.3.6 System Function Protection	23
7.3.7 Security Management	24
7.4 Management Plane Security Testing	24
7.4.1 Identification and identification	24
7.4.2 Trusted Channel	24

7.4.2.1 SSH	24
7.4.2.2 TLS	24
7.4.3 System Access	25
7.4.3.1 Access Control Security	25
7.4.3.2 Serial Port Access	25
7.4.3.3 SSH Access	25
7.4.3.4 SNMP Access	26
7.4.3.5 Web Access	26
7.4.4 Resource Allocation	26
7.4.4.1 Management Plane Protocol Prevention of Abnormal Message Attacks	26
7.4.4.2 Management Plane Protocol Prevents Denial of Service Attacks	27
7.4.5 Security Audit	27
7.4.6 System Function Protection	27
7.4.6.1 Encrypted storage of sensitive data	27
7.4.6.2 Secure Boot Function	27
7.4.6.3 Pre-installed software startup and update security	28
7.4.7 Security Management	28
7.4.7.1 Hierarchical and decentralized management	28
7.4.7.2 Insecure Configuration Check	28
7.4.7.3 Digital Certificate Management	28
Reference	29

Foreword

This document is in accordance with the provisions of GB/T 1.1-2020 "Guidelines for standardization work Part 1: Structure and drafting rules for standardization documents" Drafting.

This document is Part 2 of GB/T 46240 "Technical Requirements and Test Methods for IPv6 Network Equipment Security".

The following parts were published.

- Part 1: Routers;
- Part 2: Switches.

Please note that some of the contents of this document may involve patents. The issuing organization of this document does not assume the responsibility for identifying patents.